REMARKS

Claims 1-32 are pending in the present application. It should be noted that claims 18-32 were added in the response dated April 17, 2007; however there is no reference to the examination of these claims in the latest Office Action. Applicant believes that the present application is in condition for allowance, and respectfully requests reconsideration of the rejection in light of the remarks set forth below.

I.   REJECTION UNDER 35 U.S.C. §102

The Office Action rejected claim 17 under 35 U.S.C. §102(b) as being allegedly anticipated by U.S. Patent No. 5,371,794 issued to Diffie. The rejection is respectfully traversed in its entirety.

To anticipate a claim under 35 U.S.C. § 102(b), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the … claim." (see MPEP §2131).

The Office Action states that Diffie teaches every element of claim 17.   Applicant respectfully disagrees with the characterization of Diffie for the following reasons.

Diffie discusses a method for providing a secure wireless communication link between a mobile nomadic device and a base computing unit. Diffie teaches a key change protocol between a mobile nomadic device and a base computing unit to prevent service type attacks. (Col. 10, lines 22-64). A change key message exchange may be initiated between either the base unit or the mobile device. Each participant in the protocol of Diffie generates a public key/private key pair. "The private key is kept securely by the owner of the key pair. The public

key is submitted over a secure channel to a trusted Certification Authority (CA). The CA examines the relevant information to ascertain that the public key is indeed being presented by someone whose identity is known and who can be "trusted". Having submitted the public key, *the person submitting is assumed to be in a position to obtain credentials on behalf of the machine whose public key is being certified*. The CA will then issue a certificate to the person (who is acting on behalf of the machine). The certificate will contain a binding between the public key and a logical identifier of the machine (such as a machine name), in the form of a document digitally signed using the CA's private key." As the person submitting *the public key is assumed to be in a position to obtain credentials on behalf of the machine whose public key is being certified*, Diffie merely ensures a secure communication, it *does not authenticate* the subscriber. The secure communication in Diffie could be with anyone. (See Col. 6, lines 1-17)

By contrast, the present claimed invention is aimed at an apparatus for *authenticating* a subscriber in a wireless communication system. The apparatus selectively generates "a secondary signature that is received from the mobile station". Applicant submits that "authentication" as claimed is distinct from the key change protocol described by Diffie. With authentication the verifier or apparatus is able to determine whether the mobile user device is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, Diffie fails to disclose the claimed authentication method.

Additional, upon further review of the portions cited in the Office Action, there seems to be nothing in Diffie to even suggest a method for *authenticating* a subscriber by "generating a primary signature based upon a key that is held private from the mobile station and *a secondary*

signature that is received from the mobile station" as claimed. The Office Action relies on Col. 10, lines 52-64 for illustrating the limitation of generating a secondary signature as in the claimed invention. However, this section of Diffie merely indicates that the mobile device and base unit verify signatures on change key exchange messages to provide a secure communication link. If the signatures do not match, the key change message is ignored. Comparing two signatures is different than generating a primary signature as claimed. In particular, nothing in Diffie teaches that a primary signature is generated based on a secondary signature received from the mobile station. From Col. 10, lines 24-42 of Diffie, it appears that the signed information sent from the base station to the mobile station does not use any information received from the mobile station. Consequently, Diffie fails to disclose the generation of a primary signature based on a private key and a *secondary key received from the mobile station* as claimed.

Since Diffie does not teach at least the above elements of claim 17, Applicant submits that Diffie does not teach all elements of claim 17 and therefore, claim 17 is allowable. Also, Applicant added new independent claims 30, 31, and 32 corresponding to independent claim 17 in the response filed on April 17, 2007; however, there is no reference to the examination of these claims in the latest Office Action. New claims 30, 31, and 32 have substantially the same scope as claim 17. Accordingly, Applicant submits that these claims are believed to be allowable as well.

For at least the foregoing reasons, Applicant respectfully submits that Diffie does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

II.   ALLOWED CLAIMS

Applicant notes with appreciation the Examiner's allowance of claims 1-16 and request that they be promptly issued.

Claims 18-32 were added in the response dated April 17, 2007; however there is no reference to the examination of these claims in the latest Office Action dated July 9, 2007. Applicant submits these claims are in condition of allowance, a notice of allowance is kindly requested.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Date: November 9, 2007   By: /Won Tae C. Kim/
                                          Won Tae C. Kim, Reg. # 40,457
                                          (858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121

Telephone: (858) 658-5787
Facsimile: (858) 658-2502